PATENT
450117-02810

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

TITLE: PROTOCOL FOR INSTANT MESSAGING

INVENTOR: Niels MACHE

William S. Frommer
Registration No. 25,506
FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, New York 10151
Tel. (212) 588-0800

European Patent Application
"Protocol for Instant Messaging"
Sony International (Europe) GmbH
S99P5145EP00/PAE99-082TRDE
P22955

Protocol for Instant Messaging

The present invention relates to a method for the transmission of messages in a distributed system, to a computer program product for implementing such a method in a network environment as well as to a distributed system for the transmission of messages.

The present invention generally relates to the field of electronic messaging. Electronic messages in the form of e-mails or GSM short message texts are known. They rely on a store-and-forward technique where the originator of the message sends the message to a computer node. In the node the message is stored and then forwarded to other nodes until it reaches a mailbox belonging to the intended user.

Also known from prior art are dedicated gateways for transferring a message from one transfer medium (e.g. SMS) to another transfer medium (e. g. fax). Several GSM network operators and independent service providers offer functionality like this. The major disadvantage of such systems is that there are targeted at a fixed transfer task, so is from one well-defined medium into another.

Another means known from prior art is the use of inexpensive intermediate networks for transmitting messages between different locations. For example, one could send a document as an attachment of a e-mail. This combined message is sent to dedicated gateway where it is converted to fax and transmitted to the intended recipient.

From US-A-5,608,786 an unified messaging system is known. This known technique makes use of existing communication channels or networks. Part of the system relies on a data communication network forming an intermediate leg of the distribution network. Telephone communication is typically used for initial or final legs. Voice mail, E-mail, facsimiles and other message types can be received by the system for retrieval by the subscriber. Communications may be centralised and retrieval of messages can be accomplished using one of a number of separate and distinct approaches. Thus, data communication networks such as the internet can become global voice mail and facsimile mail systems.

As state of the art messaging systems like e-mail have a store-and-forward-communication structure, they have inherently problems with instant (i. e. nearly real-time) message delivery.

Furthermore nearly real-time transmission of messages implies a big number of processing systems for high message throughput.

Therefore it is the object of the present invention to provide for a technique for the transmission of messages in a distributed system enabling for a high message throughput and a decreased load on the processing units of the distributed system.

Said object is achieved by means of the features of the independent claims. The dependent claims develop further the central idea of the present invention.

According to a first aspect of the present invention a method for the transmission of messages in a distributed system is provided. A message is received from a sending client by means of a first message gateway. Meta information extracted from the received message is transmitted from the first message gateway to a message broker. A second message gateway is selected on the basis of the meta information and client profile data. The message is sent from the first message gateway to the selected second message gateway to transfer it to a target client.

The message broker can process the meta information to provide for security and authentication and returns it to the first message gateway.

The message broker can process the meta information and return it to the first message gateway such that controlled by the processed meta information the message can be sent to the selected second gateway together with the meta information.

The message itself can be converted by a message processor before it is sent to the selected second message gateway.

According to another aspect the computer program product for implementing such a method in a network environment is provided.

According to still another aspect to the present invention a distributed system for the transmission of messages is provided. The system comprises a first message gateway for the reception of messages from sending clients and for the extraction of meta information from the received messages. A message broker receives the meta information from the first message gateway, processes the meta information and returns it to the first message gateway. The system furthermore comprises a second message gateway (which can be identical to the first message gateway) for receiving the message from the first message gateway controlled by the processed meta information and for sending the message to a target client.

A client profile database can be connected to the message broker. The message broker processes the meta information on the basis of the data of the client profile database.

The message broker can furthermore provide for a security and/or authentication functionality.

A message processor can be interconnected between the first and second message gateway for processing the content (and not the meta information) of a message.

Further features, advantages or objects of the present invention will be evident for the man skilled in the art when reading the following detailed description of embodiment of the present invention taken in conjunction with the figures of the enclosed drawings.

Fig. 1 shows an example of a instant messaging system,

Fig. 2 shows a communication structure of a messaging system,

Fig. 3 shows a message and information authentication protocol,

Fig. 4 shows a symmetric representation of the process according to the present invention, and

Fig. 5a and 5b show in detail a message and information authentication protocol.

Fig. 1 shows an example of a instant messaging system. The system essentially consists of instant message brokers 2 connected to client profile databases 3, gateways for e-mail 4, gateways for GSM/SMS 6, gateways for voice mail and facsimile 5 which can communicate with each other by means of a network 1. At least one message processor 7 can process particularly the content of transmitted messages. The instant message broker 2 manages the system configuration and state, user profiles of the client profile database 3, message routing and services, accounting and security.

Fig. 2 shows the communication structure of a messaging system. A configuration comprises an originator (instant message gateway 4), a receiver (instant message gateway 5) and a message broker 2 as well as additional units. The different units of such a system may be global distributed or located at a single computation node. In the example of Fig. 2 the data flow of such a minimal messaging system is schematically depicted.

In phase 1 the originator gateway 4 receives a message from a client (i. e. a facsimile from a PSTN), prepares (extracts) meta information from the message received and sends the meta information to the message broker 2.

In phase 2 the message broker 2 determines the required message conversion and the message route according to the state of the messaging system and client (sender and receiver) profiles stored in the connected database 3. Additionally the message broker 2 can prepare message security and also indication. The modified meta information is than returned from the instant message broker 2 to the originator gateway 4.

In phase 3 controlled by the meta information the originator gateway 4 transmits the instant message (consisting of meta information and message content) to the receiver gateway 5. In case where an additional message service or message conversion is required, the instant message can be routed over an additional message processor 7.

In phase 4 the receiver gateway 5 transmits the (eventually converted) message to the client. After transmission the receiver gateway 5 sends an acknowledgement (e. g. delivery, client receipt, or non-delivery) to the message broker 2, wherein the acknowledgement controls the message flow.

Fig. 3 shows in detail the message and information authentication protocol. At first in a set-up phase one the originator gateway 4 transmits meta information to the message broker 2, wherein the meta information can be signed.

In a release phase two the message broker 2 returns transmission management information (signed).

In a transmission phase three the originator gateway 4 transmits signed instant message to the receiver gateway 5 (optionally through message processors 7).

In a authentication and accounting phase four the receiver gateway 5 returns a signed acknowledgement to the message broker 2.

As reference to figure 4 the message transmission according to the present invention will be explained by means of the graphical representation.

In step S1 the originator gateway receives a message from a sending client. In a step S2 the originator gateway extracts meta information by performing a predetermined processing. In a step S3 a communication between the originator gateway and the message broker is set up and in a step S4 the meta information extracted in step S2 is transmitted. In step S5 the message broker modifies the meta information by using client profile data from connected client profile database. In step S6 the modified meta information (managing information) is transmitted from the message broker to the originator gateway. In step S7 a communication set-up between the originator gateway and a destination gateway is effected. In step S8 the message content and the meta information are transmitted from the originator gateway to the second (destination) gateway. In step S9 the message is delivered from the destination gateway to the target client. In step S10 the destination gateway returns a communication gateway to the message broker. In step S11 the message broker sends an acknowledgement to the originator gateway.

With reference to figure 4 the message and information authentication protocol will be explained in detail.

The originator gateway sends a time synchronised communication set-up (TSCS) login key to the instant message broker. The communication is set up by the transmission of the TSCS login key C and its digests HMAC (K1, C). The instant message broker checks the TSCS login key and returns a TSCS acknowledgement key containing a session key. The TSCS acknowledgement key containing the random generated session key C_{ack} is sent to the instant message gateway (originator). Note that the different session keys are randomly generated and unique for each communication step they are applied in.

The originator gateway appends the session key to the message and sends an instant message meta information (IMI) signed with the key K1 to the message broker. The instant message meta information (IMI) is transmitted with the appended session key C_{ack} and ist digests HMAC (K1, IMI + C_{ack}). The message broker checks the instant message meta information (IMI) and inserts and modifies information in the IMI by

using user profile tables and database information. The session key is appended to the message. The message is than signed with key K2 and key K1. The broker IMI is transmitted with the broker inner digest ID (corresponding to HMAC (K2, IMI + C_{ack}). The IMI in the broker digest are signed again with key K1 (outer digest HMAC (K1, IMI + C_{ack} + HMAC (K2, IMI + C_{ack})).

The originator gateway checks the outer digest and sends an acknowledgement process broker IMI to the message broker.

Than the originator gateway set ups a communication by the transmission of the TSCS login key C and its digest HMAC (K1, C) to the message gateway (destination). The destination gateway checks the TSCS login key and returns a TSCS acknowledgement key containing a session key. Therefore the TSCS acknowledgement key containing the session key C_{ack} is sent to the originator gateway.

The originator gateway appends the session key to the message and sends an instant message signed with key K1 to the destination gateway. Therefore an instant message (IM)(i. e. message data and IMI) containing the message M is transmitted to the destination gateway.

The destination gateway checks the instant message, converts the instant message and sends an acknowledgement which is signed to the originator gateway. The session is than finished for the originator gateway.

The message is than delivered from the destination gateway to the target client (customer).

The destination gateway is than sending a TSCS login key for a communication set-up to the message broker.

The message broker checks the TSCS login key and returns a TSCS acknowledgement key containing a session key to the destination gateway. In the acknowledgement step

the destination gateway returns the broker ID (generated previously by the message broker) and a message delivery read acknowledgement and signs it with the key K1.

The destination gateway sends a broker IMI, message delivery/read acknowledgement and signs it with K1.

The message broker checks the outer digest generated by the destination gateway with the key K1, checks the returned ID by comparing it with its own (stored) previously generated ID sent to the destination gateway, processes the acknowledgement, terminates the transaction and returns the acknowledgement to the destination gateway.

The instant message meta information integrity and origin is assured by the generation of the meta information inner digest ID (by using the message broker key K2) and the comparison with the inner digest ID received from the destination gateway. Therefore the message broker can positively control the proper transmission of the inner digest ID from the sending gateway to the destination gateway. Furthermore it can be assured that no communication between the sending gateway and the destination gateway is possible without intervention of the message broker.

The message broker then sends a TSCS login key for a communication set-up to the originator gateway.

The originator gateway checks the digest, processes the acknowledgement, notifies the sending client and returns an acknowledgement to the message broker.

The message broker than transmits a transmission message delivery acknowledgement signed with K1 to the originator gateway.

The originator gateway checks the TSCS login co-key and returns a TSCS acknowledgement key containing the session key to the instant message broker.

The invention therefore provides a technique for (nearly) real-time capital flow control of direct messaging in a distributed messaging system.

The purpose of instant messaging is to transmit high priority messages in (nearly) real-time between clients (man and machine). Unified messaging merges analog and digital transmitted messages such as facsimile, voice mail, e-mail, WWW and the cell phone short message service (GSM/SMS) to unified instant messages. A Unified Instant Messaging System (UIMS) is a (global) distributed system that consists of four major components that communicate with each other over an IP network: distributed gateways, message processors message brokers and a client directory database. Messages of arbitrary form are converted into Unified Instant Messages by the Instant Message Gateways and vice versa. The Instant Message Brokers (IMB) controls the message flow, accounting and message conversion Additionally message brokers must ensure the authentication and security of instant messages to prevent the distributed system from unauthorised access.

The present invention is an efficient data transmission protocol for the transmission of messages in nearly real-time. In an UIMS a relatively small number of message brokers manages the message transfer, processing and security. Thus, the communication protocol and unified message structure is optimised for high message throughput and a minimum broker load. Instead of complete message transmission and processing, IMBs processes message meta information.

The present invention describes an apparatus and method for controlling message flow and processing in a distributed instant (i.e. nearly real-time) messaging systems. Because of the meta information is much more compact as the message itself, a higher throughput with reduced data transfer is reached. The (meta) message content and control flow is transmitted with authentication which means that it allows the communicating parties (gateways processors and brokers) to verify that the received messages (as well as the true and alleged originator) are authentic. In MIAP information is authenticated using Time Synchronised Communication Setup by Keyed-Hashing Message Authentication (TSCS) for message authentication.

Authenticated, high throughput apparatus and method (protocol) for a communication in distributed, direct messaging systems are proposed. The message flow control and

further messaging process of such a system is managed by one of several instances of message brokers. Time synchronised communication set up by keyed-hashing method authentication (TSCS) for message authentication is used.